

2022 Aviation Industry Cyber Threat Context

The aviation industry is an attractive target for malicious actors due to its crucial role in international movement of goods and people and the vast amounts of sensitive information aviation companies hold. Cyberattacks in 2022 have highlighted the fragility of aviation supply chain and business operations, as well as the potential impact that successful attacks can have. The aviation supply chain is varied and complex, with multiple global third parties, and relies on interconnected systems with numerous time-sensitive moving parts. Growing interconnectivity and heightened geopolitical tensions in the global supply chain are driving an increased risk to aviation organizations from cyberattacks.

Threats to the industry come from groups ranging from activists to cyber criminals to nation-state actors. Organizations face a host of potential business impacts, including data exfiltration, equipment damage, and operational disruption, as well as a persistent threat from nations conducting cyber espionage to steal proprietary data and intellectual property. Personally Identifiable Information (PII)—including Social Security numbers, passports, financial records, phone numbers, and addresses—is often the main target for cybercriminals targeting aviation, who leverage such data to commit fraudulent activity or sell to third parties on deep and dark web (DDW) forums.

Airlines and airports are attractive targets themselves, but the cyber threat landscape facing the aviation industry as a whole must be considered in the implementation of solutions. Operators are primarily concerned with finding efficient and cost-effective solutions to the movement of goods and people, but good cybersecurity hygiene may not compliment—and could even run contrary to—these practices. To adopt digital solutions safely, a thorough understanding of the threat landscape and of good cybersecurity practices must be obtained and considered as a key pillar in the design and maintenance processes.

> Key Findings

- Ransomware and digital extortion remain some of the greatest threats to the aviation sector and its supply chains. Threat actors may resort to more extreme pressure tactics to elicit payment from victims.
- Social engineering campaigns targeting the industry remain highly effective, with attacks in 2022 compromising both customers and employees of aviation companies and adjacent industries.
- The fall in the number of aviation industry-related advertisements from initial access brokers (IAB) on DDW forums throughout 2022 does not necessarily correspond to a reduction in threat. Illicit access to large or high-profile aviation industry entities will likely increasingly be sold via private or direct communication methods.
- Information technology infrastructure faces the greatest threat from malware, with saturated loader, infostealer, and trojan marketplaces filled with malware designed to target Windows or Linux-based systems. Aviation organizations may face an increased threat from wipers leveraged by Russia-backed entities.
- Botnets pose a significant threat to aviation organizations on two key fronts—stealing credentials and remotely controlling infected devices. Distributed Denial of Service (DDoS) attacks against the aviation industry likely have disproportionate impact, given the downstream effects of a short disruption to operations, but rarely last long or cause long-term damage.
- Aviation organizations increasingly rely on third-party vendors to provide network edge, cloud computing, and remote management technologies to enable business operations, greatly expanding the cyber attack surface.

Who is targeting Aviation?

- | | |
|---|---|
|  Financially-motivated threat actors |  Foreign governments / Nation states |
|  Politically-motivated threat actors |  Insider threats |
|  Competitors |  Activists |

Why target Aviation?

- | | |
|--|---|
|  Hold valuable data, information, and intellectual property |  High revenues and large transactions |
|  Serves as initial foothold to exploit downstream targets |  High level of access into multiple key aviation industry targets |
|  Ability to greatly impact the aviation industry and maintain plausible deniability |  Part of a controversial sector given the high cost of living and climate change |



ZeroFox Intelligence Cyber Threat Landscape: Aviation Industry 2022



TLP: CLEAR

B-2022-10-14b

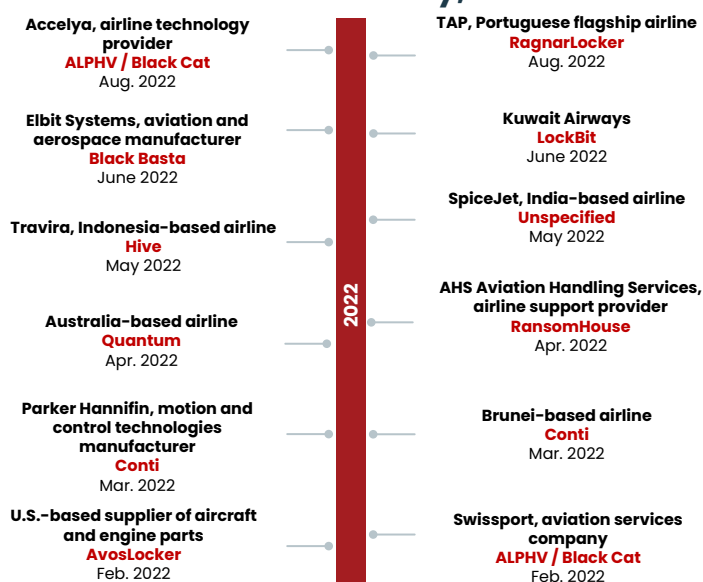
Ransomware and Digital Extortion

Ransomware and digital extortion remain some of the greatest threats to the aviation industry and its supply chains. Attacks against the aviation industry are frequent, despite a reduction in threat in 2022 compared with 2021 levels. This is likely in part caused by both disruption to threat actor operations following Russia's invasion of Ukraine and difficulty in eliciting payments from victims. Attacks against the industry often target supply chains, including equipment manufacturers, maintenance service providers, and operating systems. Attacks in 2022 have highlighted the vulnerability that stems from targeting aviation third-party providers.[1]

Financially and politically-motivated extortionists very likely view the aviation sector as an attractive target due to the wealth of customer data and personal information they hold, high revenues, and the industry's importance to national infrastructures. Attacks could negatively impact multiple dependent industries and lead to disruption in international distribution and financial loss. As an industry that relies on prompt timing and efficiency, a small delay to operations can have a disproportionate impact. Companies in the sector may be viewed as more likely to quickly pay a ransom if an attack causes sufficient disruption to operations.

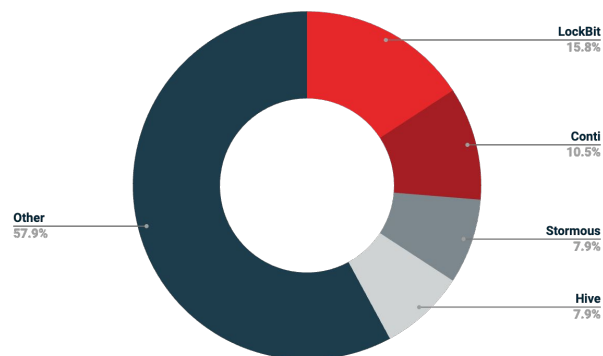
ZeroFox has identified at least 30 ransomware and digital extortion incidents targeting the industry to date in 2022, with LockBit the primary digital extortion threat and most active group.[2] Security teams should be wary of extortion operations linked to Conti and possible splinter groups, including Black Basta and Hive.[3,4] As Conti was one of the most frequent targeters of the aviation industry this year, high frequency of targeting may continue.

Selected Ransomware Attacks Impacting the Aviation Industry, 2022



Source: ZeroFox Intelligence

Groups Most Actively Targeting Aviation (Globally), 2022



Source: ZeroFox Intelligence

Extortion attacks against the aviation industry are likely to increasingly involve nation-states utilizing cybercrime collectives as a proxy. Russia has a history of leveraging cybercriminal groups to advance foreign policy goals while maintaining plausible deniability. Ransomware has also been used as a cover to mask other malicious activity, such as cyber espionage.

Recent changes to threat actor tactics in the post-exploitation stage may indicate that ransomware gangs are finding it increasingly difficult to elicit payments from victims. The supply chain risk is compounded by developments in extortion tactics, with ALPHV/BlackCat providing leaked victim data in a searchable format.[5] Threat actors have begun hacking corporate websites to display ransom notes to increase pressure on victims. LockBit began testing a new process in which it gradually reduces the ransom demand, hoping victims that initially refuse to pay may decide it is financially prudent to recover stolen data at a lower price. Should difficulty obtaining ransom payments remain, threat actors may resort to increasingly extreme pressure tactics. LockBit victims may face greater threat from DDoS attacks as an additional pressure tactic, which could have a disproportionate impact on organizations in the aviation industry.[6]

Forward Look:

- The aviation industry is likely to be increasingly targeted by extortion groups with alleged links to Conti, given its former tendency to target the industry.
- Threat actors may resort to more extreme pressure tactics to elicit payment from victims, causing greater operational downtime, reputational damage, and legal ramifications.

Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate Indicators of Compromise (IOCs) and metadata related to Malware and Ransomware.
- Should an organization be impacted by a ransomware event, engage ZeroFox Intelligence for support.

FOOTNOTES

- [hXXps://www.scmagazine.com/brief/ransomware/alphv-ransomware-hits-accelya](https://www.scmagazine.com/brief/ransomware/alphv-ransomware-hits-accelya)
- ZeroFox Intelligence Internal Collections
- [hXXps://www.computerweekly.com/news/252521980/Black-Basta-ransomware-crew-aiming-for-big-leagues](https://www.computerweekly.com/news/252521980/Black-Basta-ransomware-crew-aiming-for-big-leagues)
- [hXXps://www.wired.com/story/costa-rica-ransomware-conti/#:text=Conti%20claimed%20responsibility%20for%20the,impacting%20the%20health%20care%20system](https://www.wired.com/story/costa-rica-ransomware-conti/#:text=Conti%20claimed%20responsibility%20for%20the,impacting%20the%20health%20care%20system)
- [hXXps://krebsonsecurity.com/2022/06/ransomware-group-debuts-searchable-victim-data/](https://krebsonsecurity.com/2022/06/ransomware-group-debuts-searchable-victim-data/)
- [hXXps://www.itworldcanada.com/article/lockbit-ransomware-gang-adding-ddos-attacks-to-its-threats/500301](https://www.itworldcanada.com/article/lockbit-ransomware-gang-adding-ddos-attacks-to-its-threats/500301)



Social Engineering

Social engineering is one of the most frequently reported cybersecurity threats leveraged against the aviation industry, indicating human error remains a barrier to effective security practices. Campaigns continue to target both customers and employees of aviation and its adjacent industries.[7,8] This is expected to remain the case for the foreseeable future; campaigns are demonstrably effective, enabling threat actors to steal credentials, deploy follow-on payloads, and conduct financial fraud.

Social engineering against the industry remains evolutionary rather than revolutionary. ZeroFox Intelligence identified a number of campaigns aimed at aviation this year, including payment scams directed at customers or attempts to harvest credentials from employees via phishing emails, text messages, and voice calls.[9] Threat actors are most likely to leverage topical lures and some element of time constraint to entice customers and employees to enter credentials in phishing domains or to execute malicious attachments to emails. Hiring managers and job-seekers have also been targeted in employment-related scams, facilitating financial loss, malware deployment, and acquisition of privileged access.[10]

Although not exclusive to the aviation sector, industry organizations should note recent developments of threat actors increasingly leveraging smishing attacks, callback phishing to add legitimacy to malicious emails by impersonating security teams, and techniques to bypass multi-factor authentication (MFA).

Forward Look:

- Smishing of aviation organizations' employees and customers is likely to continue on an upward trajectory.
- Threat actors are very likely to increasingly leverage MFA-bypassing social engineering techniques.

Recommendations:

- Impersonation phishing domains and open redirects, which provide intrusion vectors for threat actors, should be continually monitored and taken down to prevent customers from being defrauded.
- Engage the ZeroFox Intelligence Team to conduct an Attack Surface Assessment to understand the threat posed to your organization.

Case Study: Phishing Campaign Leveraging Employees' Accounts

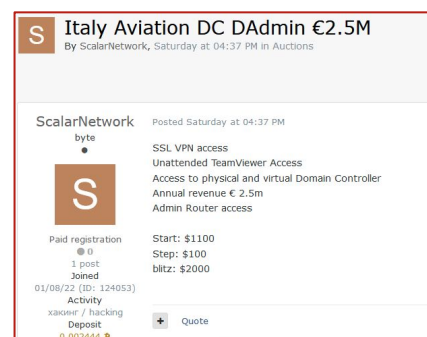
In September 2022, American Airlines (AA) disclosed a data breach from July 2022, which was discovered after compromised Microsoft 365 employee email accounts were leveraged in phishing attacks.[11] After compromising an AA employee's account, the attacker accessed multiple other accounts and used them to send further phishing emails to other undisclosed targets. AA stated that, while personal information of 1,708 customers and employees were contained in the mailboxes, it had not yet seen evidence of data misuse. While only minor impacts seem to have occurred, an undetected attacker in a large conglomerate's internal systems for months could have had a catastrophic impact on operations.

Initial Access Brokers

Aviation industry-related advertisements from IABs (initial access brokers) on DDW forums have decreased throughout 2022, but this does not necessarily correspond to a reduction in threat. It instead likely reflects ongoing limitations to the supply of advertisements on forums due to a confluence of factors, including IABs being implicated in Russia's invasion of Ukraine and threat actors choosing more private means of communication to sell illicit access by leveraging well-established relationships with specific buyers rather than advertising in open forums. The IAB ecosystem operates on reputational currency; although motivated by profit, brokers are reluctant to sell access to unknown or untrusted actors.

Access to aviation firms posted in open channels is most likely to target airlines of European, South American, and Asian nations or upstream aviation suppliers, such as manufacturers. Access to targets that are deemed more lucrative or higher profile will likely be sold in private channels. IABs will almost certainly continue to gain network access to aviation organizations in a bid to cater to ransomware groups' appetite to strike lucrative aviation targets.

Acquiring access through IABs can be inexpensive and target small organizations. In May 2022, untested threat actor "ScalarNetwork" advertised Teamviewer remote desktop and SSL VPN access to the internal network of an Italian aviation company.[12] ScalarNetwork claimed to have administrator rights to a domain controller and router on the network and that the company generated USD 2.6 million in revenue. The actor auctioned the access with a starting bid of USD 1,100 and an instant purchase price of USD 2,000.



Source: ZeroFox Intelligence

Forward Look:

- Illicit access to large or high-profile aviation industry entities will likely increasingly be sold via private or direct communication methods.

Recommendations:

- Employ ZeroFox's Threat Intelligence Feeds to proactively monitor for potential network access sales and obtain critical early warnings of impending cyberattacks.

FOOTNOTES

[7] <https://twitter.com/UCConviasa/status/1514802809886273540?s=20&t=2Ti-hoUwii-WQM3Pn-w>

[8] <https://sturbone.com/united-airlines-com-urgent-fraud-warning/>

[9] <https://swordtoday.com/fake-plane-ticket-fraud-on-facebook/>

[10] https://www.reddit.com/r/americanairlines/comments/tq655/scam_job_offer_its_saying_i_have_to_pay_like_100/

[11] <https://www.bleepingcomputer.com/news/security/american-airlines-discloses-data-breach-after-employee-email-compromise/>

[12] ZeroFox Intelligence Internal Collections



ZeroFox Intelligence Cyber Threat Landscape: Aviation Industry 2022



TLP: CLEAR

B-2022-10-14b

Malware

ZeroFox Intelligence assesses with low confidence that the threat of malware deployment against the aviation industry in 2022 has remained broadly consistent with 2021 levels. Malware deployment across the landscape has remained highly prevalent throughout 2022, and ZeroFox Intelligence expects that to continue given ease of acquisition and impact on end users. While infection rates remained high, ZeroFox Intelligence has observed no significant changes in malware capability.

IT infrastructure faces the greatest threat, with saturated loader, infostealer, and trojan marketplaces filled with malware designed to target Windows or Linux-based systems. Threat actors identified in 2022 are known to leverage remote access trojans, including AsyncRAT, to obtain control over devices and exfiltrate sensitive information.[13] The threat is unlikely to reduce in the near term given the ease of acquisition and potential impact, with Malware-as-a-Service (MaaS) models maintaining low barriers to entry. The proliferation of mobile malware remains high and is leveraged both as a means to steal passwords, banking information, and other sensitive user information and to intercept MFA codes. Dissemination of malware via fake apps on application marketplaces also continues to rise, increasing the potential risk for those that use personal devices professionally.

If Russia's focus reverts to its other long-standing interests, wiper malware leveraged during Russia's invasion of Ukraine, or variants of these strains, the aviation industry will likely be an attractive target through which to cause widespread disruption.[14] A wiper attack against a single aviation target could have significant global impact. To date, wiper malware leveraged during the conflict has largely been limited to use in Ukraine and the immediate surrounding area. A shift in focus could see these strains deployed more broadly against aviation targets in Western nations; those who vocally opposed Russia's actions; pro-European Union nations; and other nations in Russia's geographic proximity.

Forward Look:

- MaaS offerings will very likely sustain low barriers to entry for threat actors and drive down the price of acquiring highly-capable malware.
- Threat actors operating the most effective trojans will almost certainly continue to rapidly update capabilities to take advantage of vulnerabilities in widely-used software, placing increased importance on having a comprehensive and efficient patching program.

Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate IOCs and metadata related to Malware and Ransomware.

Botnets and Denial of Service

Botnets pose a significant threat to aviation organizations on two key fronts: stealing credentials and remotely-controlling infected devices. Once a device is infected by malware and forced into being part of a botnet, the malware harvests credentials—including from Internet-of-Things (IoT) devices. Credentials harvested are often sold or traded on the dark web for a profit and reused by extortion groups to gain initial access inside a corporate network.

ZeroFox Intelligence analyzed the top 10 global airlines (by revenue) and identified systems infected with various credential-stealing malware families; more than 37,000 login credentials were exfiltrated from these companies in 2022 alone.[15,16] These compromised systems yield stolen user data in the form of botnet logs and contain login credentials and additional system information, such as browser cookies—increasing the likelihood of phishing, spam, and onward fraud operations targeting airline users. Threat actors that purchase this data potentially gain access to the entirety of a victim's login credentials and cookies, which allows them to emulate the victim's browser session and user agent to achieve unauthorized access in account takeover attacks.

Threat actors leveraging infected devices for DDoS attacks against the industry have been highly prevalent in 2022, particularly against airline websites and airport operations.[17] DDoS attacks against the aviation industry likely have disproportionate impact, given the downstream effects of a short disruption to operations. However, despite receiving widespread media attention, DDoS attacks rarely last long or cause long-term damage.

DDoS attackers are most likely to be politically motivated, as reflected in incidents targeting high-profile political events such as Russia's war in Ukraine and Nancy Pelosi's visit to Taiwan.[18] Killnet, one of the most vocal threat groups since the start of Russia's invasion of Ukraine, has targeted airport infrastructure across Europe and the United States throughout 2022—most recently in October 2022 attacks against airport websites in at least 24 different U.S. states.[19] Killnet's attacks are typically short and are used to increase the group's publicity. Threat actors could instead be financially-motivated, launching ransom DDoS (RDDoS) by threatening organizations with DDoS attacks unless an extortion demand is paid. Ransomware and extortion collectives also leverage DDoS attacks as part of triple extortion tactics to increase pressure on victims to fulfill ransom demands.

Forward Look:

- Expansion of the botnet market will continue, with new botnets emerging to target web servers, modems, routers, IoT, and Android devices.

Recommendations:

- Subscribe to the ZeroFox botnet and compromised account alerts to identify any exposure of employee or customer credentials in the wild.

FOOTNOTES

- [13] <https://threatpost.com/loader-aviation-spy-rats/166133/>
[14] <https://www.techtimes.com/articles/273755/20220331/viasat-hit-russia-s-wiper-malware-called-acidrain-affecting-european.html>
[15] <https://www.altoeverything.com/top-10-biggest-airlines-in-the-world/>
[16] ZeroFox Intelligence Internal Collections
[17] <https://www.bankinfosecurity.com/pro-russian-killnet-group-in-ddos-attacks-on-czech-entities-a-18949>
[18] <https://www.nbcnews.com/tech/security/taiwanese-websites-hit-ddos-attacks-pelosi-begins-visit-rcna41144>
[19] <https://www.bleepingcomputer.com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers/>



Third-Party Vulnerabilities

Organizations within the aviation industry are very likely becoming less self-contained and increasingly collaborating with industry partners to deliver services. Companies themselves increasingly rely on third-party vendors, not only to provide equipment and management services but also to provide network edge, cloud, and remote management technologies to enable operations. While this has made organizations more efficient, it has expanded the cyber attack surface, as threat actors can leverage trusted access afforded to external entities to target downstream targets.

The adoption of third-party solutions drives progress in terms of efficiency, automation, remote management, and data analytics. However, such solutions also provide threat actors with additional attack vectors; vulnerabilities in devices used by a single entity can be leveraged to target entire supply chains. Differing levels of security among third parties also make them ideal targets for threat actors. There is also a multiplier effect: in a multi-tier supply chain, one intrusion can create a platform from which threat actors can compromise the systems of hundreds—or thousands—of end users.

ZeroFox Intelligence identified a number of third-party compromises impacting aviation and adjacent industries in 2022. These include delays to a Canadian airline's operations following a hack of a third-party system the airline uses, a breach of a military manufacturing contractor putting the Canadian government on high alert, and a breach of a third-party vendor impacting Boeing Employees' Credit Union.^[20,21,22] The threat from compromise via third-party services is expected to continue on an upward trajectory.

Forward Look:

- Threat actors will continue to target the supply chain through proprietary source code, developer repositories, and open source libraries and will continue to leverage high-profile vulnerabilities in widely-used software, such as the Follina, Confluence, and F5 BIG IP applications, long after the security patches were released.

Recommendations:

- Integrate ZeroFox tactical threat intelligence into supply chain management and actively engage in third-party monitoring.
- Engage in ZeroFox proactive investigations of cybersecurity risks associated with new suppliers and vendors prior to their onboarding.
- Taking a reactive approach to third-party cyber risk can make it difficult to respond to incidents in a timely manner. Establish cybersecurity accountability throughout the supply chain and regularly assess high-value assets.

APPENDIX: Traffic Light Protocol for Information Dissemination

TLP: RED

HOW IT IS USED

Sources may use **TLP: RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share **TLP: RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP: AMBER

HOW IT IS USED

Sources may use **TLP: AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share **TLP: AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP: AMBER+STRICT restricts sharing to the organization only.

TLP: GREEN

HOW IT IS USED

Sources may use **TLP: GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share **TLP: GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP: CLEAR

HOW IT IS USED

Sources may use **TLP: CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share **TLP: CLEAR** information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox provides enterprises protection, intelligence, and disruption to dismantle external threats to brands, people, assets, and data across the public attack surface in one comprehensive platform. With complete global coverage across the surface, deep and dark web and an Intel-backed artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, ransomware, brand hijacking, executive and location threats, and more. The patented ZeroFox Platform technology processes and protects millions of posts, messages, and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email, and more.

Ready To See For Yourself?

Request a Demo:

Sign up on zerofox.com/request-a-demo

Learn More:

Visit zerofox.com

Contact us at sales@zerofox.com / 855.736.1400

FOOTNOTES

[20] <https://www.infosecurity-magazine.com/news/cyberattackers-hit-sunwing-airlines/>

[21] <https://globalnews.ca/news/8906423/national-defence-potential-impacts-cyberattack-military-contractor/>

[22] <https://media.dojmtl.gov/wp-content/uploads/Consumer-Notification-Letter-427.pdf>

